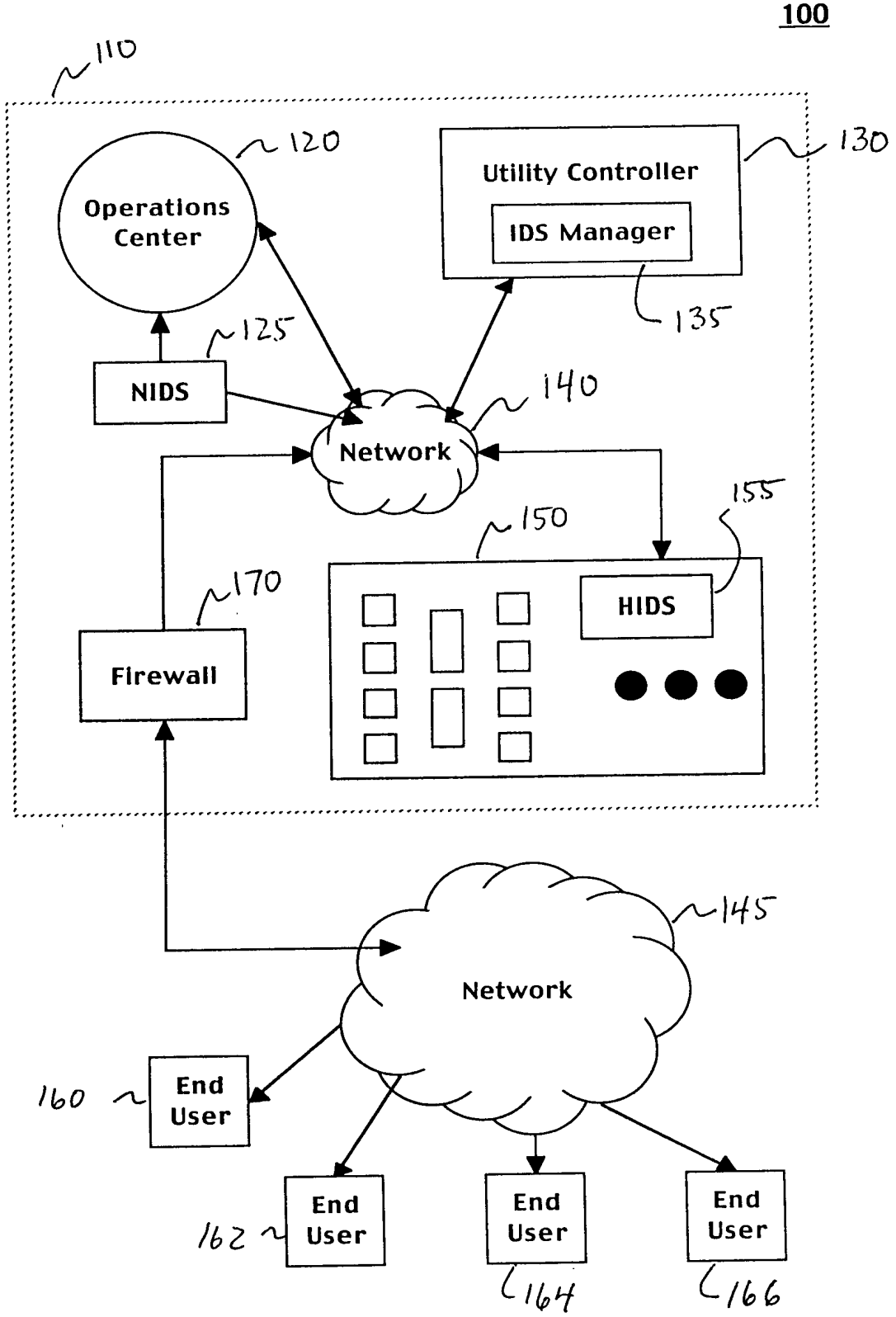
100
110
120
Operations Center
130
Utility Controller
IDS Manager
135
125
NIDS
140
Network
150
155
HIDS
170
Firewall
145
Network
160
End User
162
End User
End User
164
End User
166

Fig. 1

200

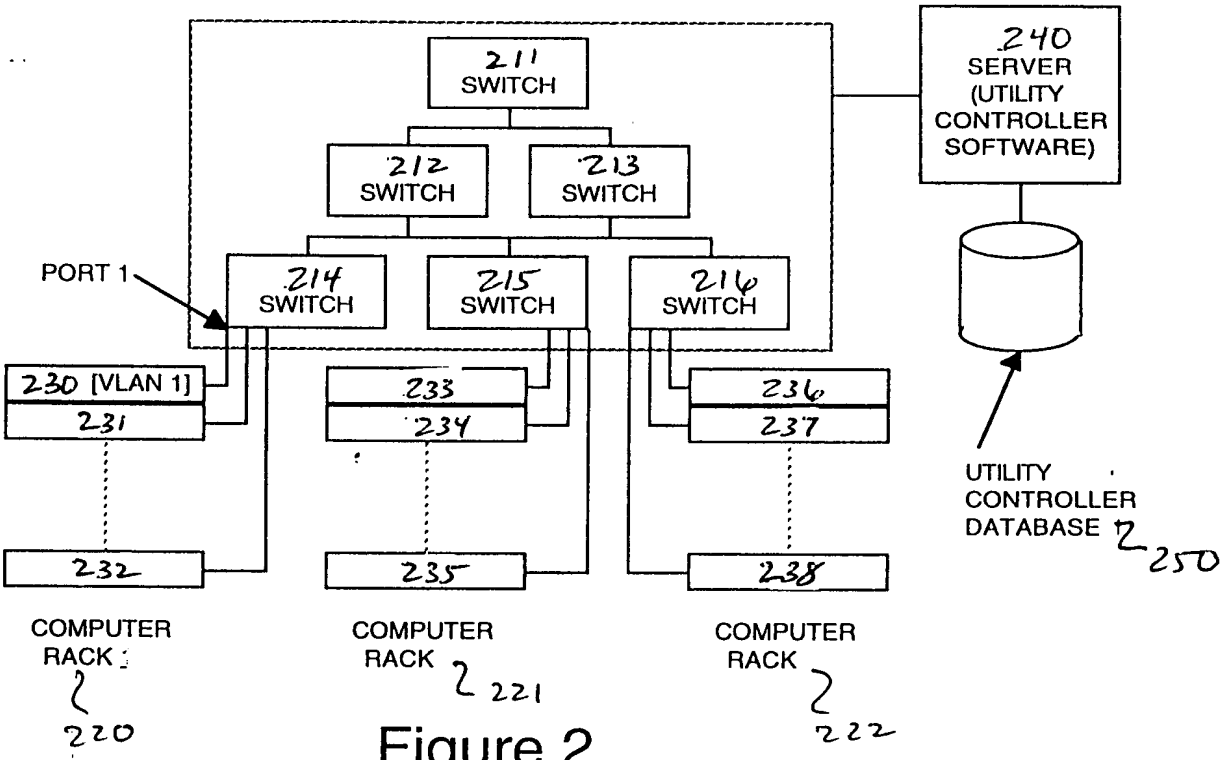
211
SWITCH
212
SWITCH
213
SWITCH
214
SWITCH
215
SWITCH
216
SWITCH
PORT 1
240
SERVER
(UTILITY
CONTROLLER
SOFTWARE)
230 [VLAN 1]
231
233
234
236
237
232
235
238
UTILITY
CONTROLLER
DATABASE
250
COMPUTER
RACK
220
COMPUTER
RACK
221
COMPUTER
RACK
222

Figure 2

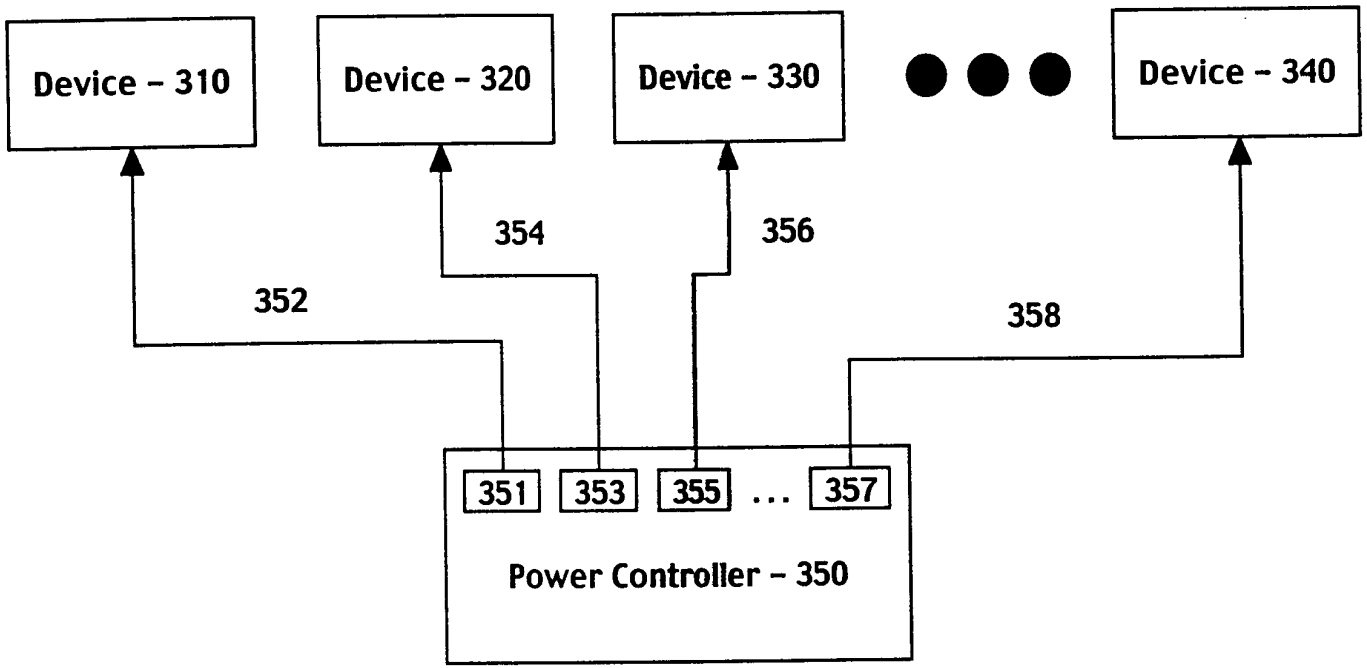
300
Device – 310
Device – 320
Device – 330
Device – 340
352
354
356
358
351
353
355
...
357
Power Controller – 350

Fig. 3

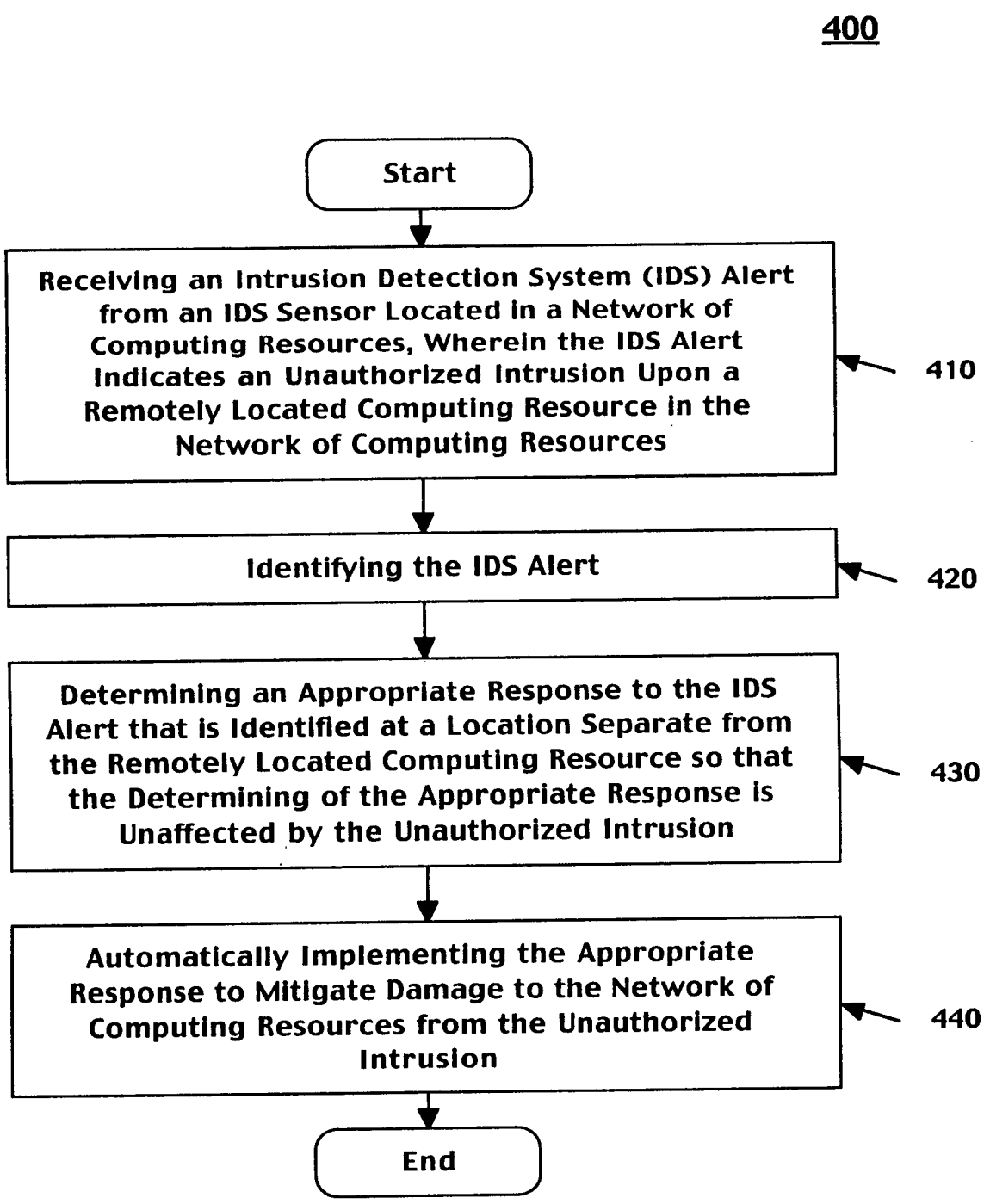
400
Start
Receiving an Intrusion Detection System (IDS) Alert from an IDS Sensor Located in a Network of Computing Resources, Wherein the IDS Alert Indicates an Unauthorized Intrusion Upon a Remotely Located Computing Resource in the Network of Computing Resources
410
Identifying the IDS Alert
420
Determining an Appropriate Response to the IDS Alert that is Identified at a Location Separate from the Remotely Located Computing Resource so that the Determining of the Appropriate Response is Unaffected by the Unauthorized Intrusion
430
Automatically Implementing the Appropriate Response to Mitigate Damage to the Network of Computing Resources from the Unauthorized Intrusion
440
End

Fig. 4

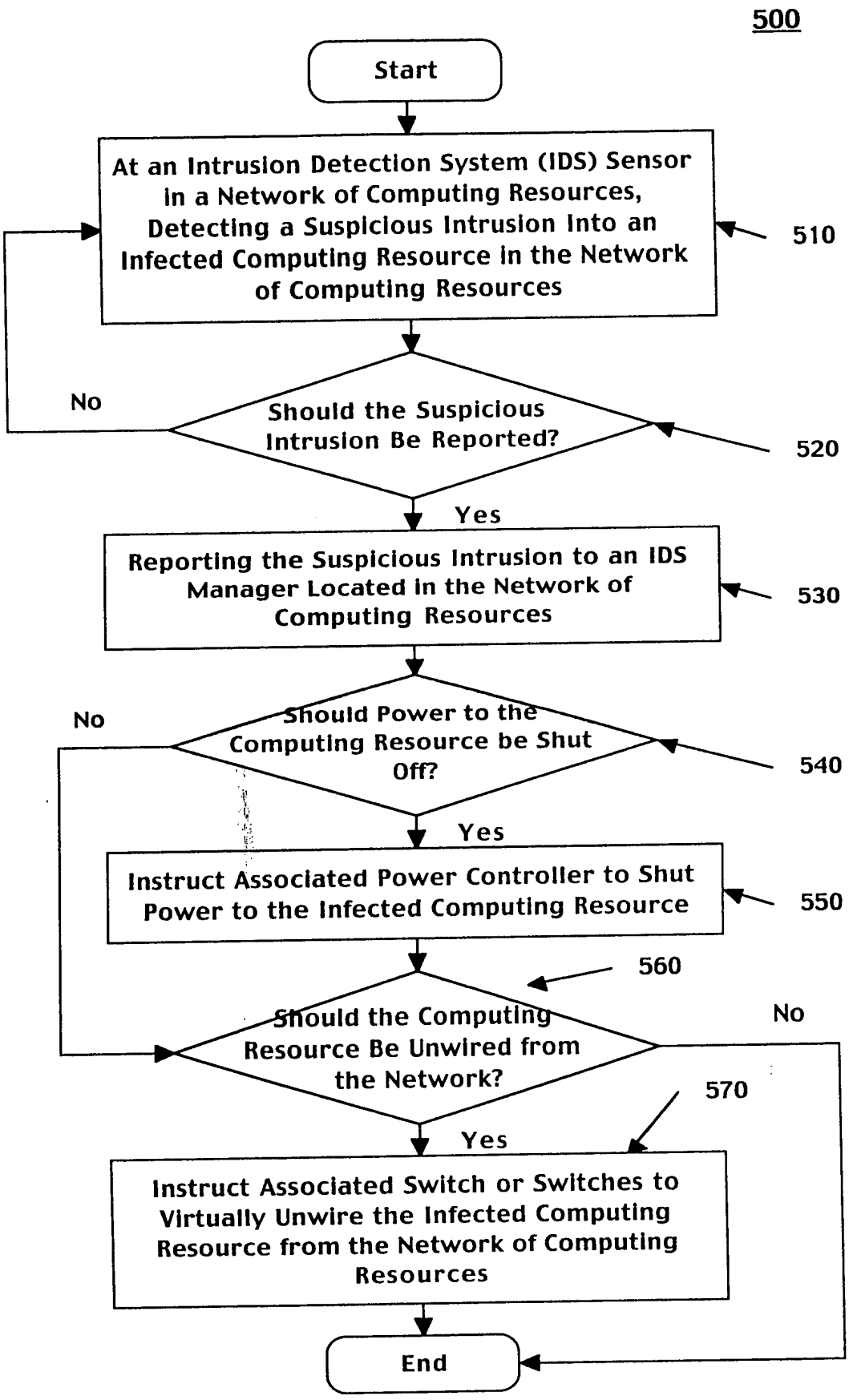
500
Start
At an Intrusion Detection System (IDS) Sensor in a Network of Computing Resources, Detecting a Suspicious Intrusion Into an Infected Computing Resource in the Network of Computing Resources
510
Should the Suspicious Intrusion Be Reported?
520
No
Yes
Reporting the Suspicious Intrusion to an IDS Manager Located in the Network of Computing Resources
530
Should Power to the Computing Resource be Shut Off?
540
No
Yes
Instruct Associated Power Controller to Shut Power to the Infected Computing Resource
550
560
Should the Computing Resource Be Unwired from the Network?
No
570
Yes
Instruct Associated Switch or Switches to Virtually Unwire the Infected Computing Resource from the Network of Computing Resources
End

Fig. 5